

Forbes / Asia / [#CyberSecurity](#)

FEB 14, 2018 @ 12:36 AM

1,761 👁

# How The \$500 Million Coincheck Hack Exposes Deeper Security Flaws In Corporate Japan

**Tim Romero**, CONTRIBUTOR[FULL BIO](#) ✓

Opinions expressed by Forbes Contributors are their own.

## TWEET THIS



Japanese engineers who alert their firms to security flaws are often taking significant career risk in doing so.



the Japanese language itself provided an effective layer of obfuscation over poor security practices



Shutterstock

Last month hackers stole more than \$500 million in cryptocurrency from Coincheck, one of the largest crypto exchanges in Japan. There has already been a lot of coverage of what happened and what Coincheck promises to do about it.

I would like to explain why it happened, and why it is likely to happen again.

Japan has always been, and still remains, a soft-target for cybercrime. Security problems are systemic and deeply interwoven in Japanese business culture. In the past, Japanese IT systems have been largely spared due to a unique combination of linguistic and system isolation that is now coming to an end.

Corporate Japan has a strange relationship with computer security. On one hand, firms pay top dollar for security hardware, consulting, and compliance audits. On the other, however, practical security is frequently neglected. Operating systems remain un-patched, firewalls are never changed after initial configuration, and backup systems are rarely tested.

### **Security's Serious Not-My-Problem Problem**

I've worked with dozens of Japanese companies over the years, from small startups to Global 500 corporations. In only a handful of cases has the person in charge of IT security had a background in the field.

Part of the problem stems from the hierarchal nature of Japanese society where management experience is valued more highly than domain expertise, coupled with the fact that the domain of computer security changes so rapidly.

### **More On Forbes:** *Coincheck Hack Could Be The World's Biggest Ever Crypto Theft*

“Most Japanese CIOs and Chief Security Officers (CSOs) are in their 50s, but these positions are much more junior than in the West,” explains Atsuyoshi Shimazu, CEO of Japanese security startup Caulis. “CSOs are expected to be skilled at managing technology projects but are not generally expected to have a technical background. Japanese firms have a history of outsourcing their systems, so they often lack this kind institutional knowledge.”

This situation has led to compliance being valued far more than actual security in Japan.



Officials from the Financial Services Agency arrive at Coincheck's Tokyo headquarters to conduct a search on February[+]

## It's Not a Problem If We Don't Admit It

It's difficult being the bearer of bad news in any culture, but Japanese engineers who alert their firms to security flaws are often taking significant career risk in doing so.



The strong social stigma attached to speaking out against the group, the lack of technical understanding and the absence of any immediate consequences to poor security, results in engineers who raise security concerns being viewed as disruptive at best, and troublemakers at worst.

Documenting, or even fixing, security vulnerabilities provides no immediate benefit. Senior management does not have the background to understand either the risks involved or to evaluate improvements once they are made. They are, however, all too aware of the budget that mitigation efforts consume, the projects that they delay and the resources that must be diverted once a serious security concern has been documented.

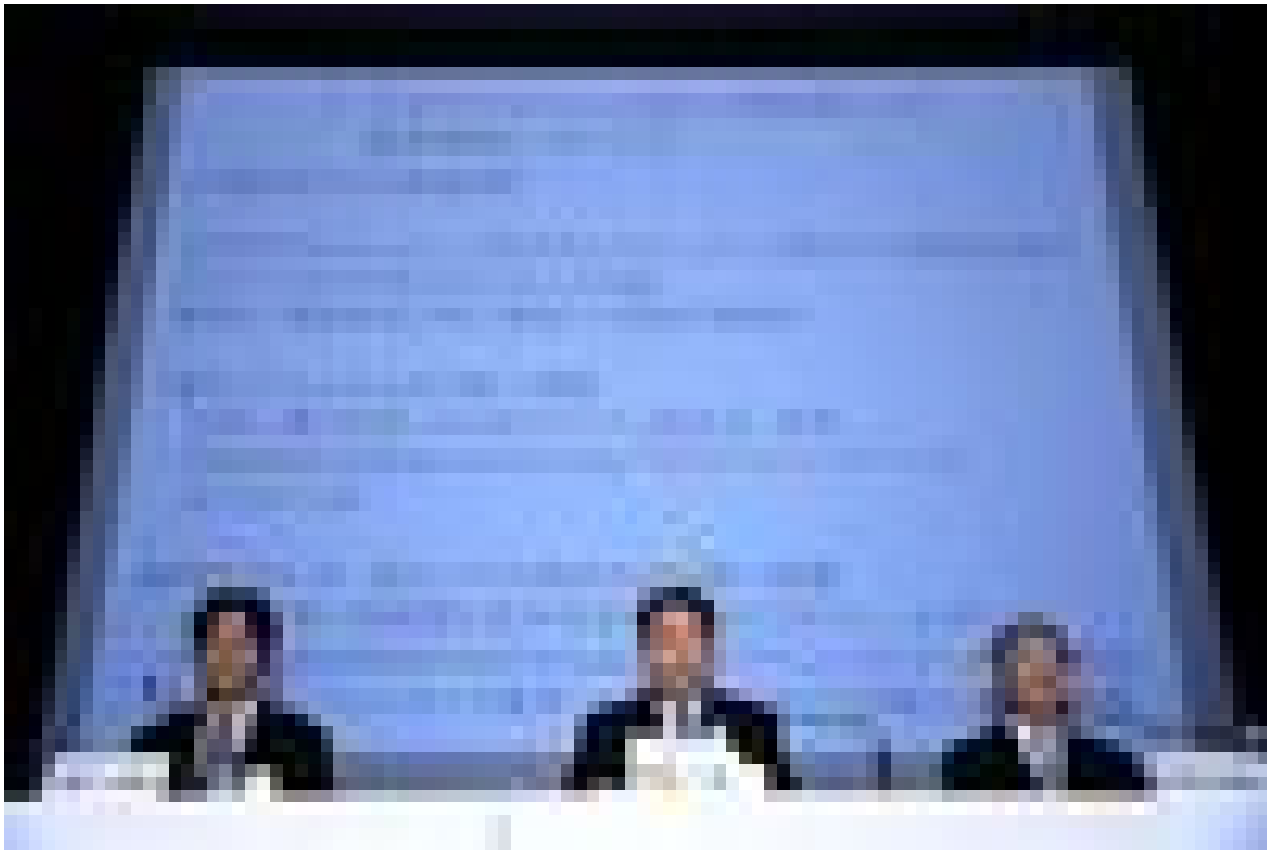
**More On Forbes:** [11 Cybersecurity Resolutions For 2018](#)

As a result, many Japanese companies handle new security concerns informally. If there are resources available, the vulnerabilities will be formally documented and

addressed. If not, they remain officially unknown and no one individual will be held responsible for them.

To be fair, we see the same pressures in large organizations all over the world. In Japan, however, the same dynamic frequently plays out even in small startups.

While more and more engineers are starting companies in Japan, Japanese investors strongly prefer and overwhelmingly fund founders with a background in finance or management consulting. Japanese startups often have the in-house technical expertise that enterprises lack, but they frequently fall into the same security groupthink as their larger brethren.



*Sony executives were forced to apologize in 2011 for the massive theft of personal data from users of the company's* [ + ]


The effects are visible in the Japanese marketplace. Since startups and enterprises both tend to favor compliance over detection and mitigation, there is a wide range of security audit and consulting services available, but penetration testing is rare and expensive.

Similarly, most Western technology companies sponsor “bug bounty” programs where they offer cash rewards to honest hackers who discover and report security flaws. Few Japanese firms of any size are willing to open themselves up to such public scrutiny.


Computer security remains something that must be handled quietly and out of sight.

## Why Things Are About To Get So Much Worse

With the poor state of security in Japan, it might seem surprising how little cybercrime there actually is. For example, the National Police Agency (NPA) reports \$120 million in credit card fraud in Japan compared to about \$8.5 billion a year in the U.S. The Japanese economy is 30% the size of the U.S. but only has about 1.5% of the credit card fraud.

Until recently, Japan-only payment systems and the Japanese language itself provided an effective layer of obfuscation over poor security practices  and made attacks difficult. Since most cybercrime is cross-border, Japanese APIs, websites, error messages and even the data itself was unreadable by non-Japanese speakers.

The widespread availability of free, automatic translation tools has changed this. In a 2015 NPA survey of public Japanese companies, more than a third reported that they had suffered some degree of harm from these kinds of attacks. The NPA also reports that while crime is down overall in 2017, cybercrime is at record levels and increasing steadily.

Corporate Japan is becoming more vulnerable to cyber attacks at the very time they are moving more and more valuable information onto Internet-connected computers. 

Unfortunately, it looks like things will have to get a lot worse before they get better. It will take a few more expensive and embarrassing hacks the scale of Coincheck before Japan stops viewing them as isolated incidents and begins treating computer security as the serious and systemic problem it truly is.

I'm a Tokyo-based founder, consultant, author, and teacher and host the [Disrupting Japan podcast](#). I also teach corporate innovation at NYU's Shinagawa campus.